

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Applicant(s): INOUE, et al

Serial No: 08/904,137

Filed: July 31, 1997

Title: PPROGRAM WRITABLE IC CARD AND METHOD THEREOF

Group: 2132

Examiner: G. Barron

COPY

**REPLY BRIEF**

Assistant Commissioner for Patents  
Washington, D.C. 20231

January 21, 2003

Sir:

The following is in reply to the Examiner's Answer dated November 18, 2002.

**NEW POINTS OF ARGUMENT**

1. The Examiner does not agree with Appellants' statement that the claims do not stand or fall together being that the Examiner alleges that the independent claims rely on the same features to overcome Hirokawa (U.S. Patent No. 4,827,512).
2. The Examiner improperly contends that instruction data is an encrypted program being input to the IC card.
3. The Examiner contends that Appellants' characterization of Hirokawa as simply providing a system where new programs may added, without consideration for the need for security, would place Hirokawa in a position whereby the need for security would be unnecessary as users would simply be allowed to add

any program or data desired.

## **ARGUMENTS**

With respect to the first new point of argument raised by the Examiner wherein the Examiner does not agree with Appellants' statement that the claims do not stand or fall together being that the Examiner alleges that the independent claims rely on the same features to overcome Hirokawa the following is provided:

In the Appeal Brief, Appellants' properly argued that the Board should consider each of the claims individually and separately so as not to stand or fall together. In support of this statement Appellants' provided various arguments as to the differences between each of the features recited in each of the claims relative to Hirokawa. Each of these arguments regarding different features of each of the claims must be considered by Board relative to the prior art utilized by the Examiner to reject the claims in order to determine whether each individual claim is patentable.

It is quite clear by case law that the question regarding whether claims should stand or fall together is not whether the claims contain common features but whether the features that are not common in the claims render each individual claim patentably distinct relative to the other claims. Appellants' have specifically argued each of the features of each of the claims and have shown how each of the features of each of the claims even beyond those that may be common are not taught or suggested by Hirokawa. It is Appellants' position that each of the features of each of the claims which are not common to the other claims render the claims patentably distinct relative to the other claims. Thus, the claims do not stand or fall together.

The Examiner has not shown at any point in the Examiner's Answer how the features that are not common between the independent claims are obvious relative

to each other. It is Appellants' position that these features which are not common with respect to the independent claims are not obvious relative to the features that are common.

With respect to the second new point of argument wherein the Examiner improperly contends that instruction data is an encrypted program being input to the IC card, the following is provided:

Appellants' submit that the Examiner's statement regarding instruction data being an encrypted program is entirely wrong and simply ignores the plain meaning of instruction data as described in Hirokawa. Instruction data as taught in Hirokawa is simply an instruction which causes the IC card to perform a particular function. The instruction data is not a function or program that is to be added to the IC card. Column 1, lines 25-28 of Hirokawa merely describes the well known features of an IC card receiving encrypted instruction data. As per Hirokawa, in order to maintain security the instruction data is encrypted when input to the IC card and then decrypted by a decryption function stored on the IC card for processing by the functions/processes implemented by a function program when executed.

The key point to recognize here, that the Examiner seems to overlook, is that Hirokawa confirms what is known by those of ordinary in the art that encrypted instruction data is used to cause the IC card to perform a particular function, that instruction data is not an encrypted program, that the encrypted instruction data is simply data used during processings executed on the IC card, and that the encrypted instruction data is not a program to be added that is stored in the second memory of the IC card and executed by the microprocessor of the IC card.

Thus, the encrypted instruction data as specifically taught by Hirokawa is not a program to be added to the IC card wherein the program is executable and later

executed by the processor on the IC card as in Appellants' invention.

With respect to the third new point of argument raised by the Examiner wherein the Examiner contends that Appellants' characterization of Hirokawa as simply providing a system where new programs may be added, without consideration for security, would place Hirokawa in a position whereby the need for security would be unnecessary as users would simply be allowed to add any program or data desired the following is provided:

From the above allegation by the Examiner, it would seem that the Examiner would now recognize the point of Appellants' invention. Appellants' invention has been specifically described throughout the specification and claims thereof and, argued during several interviews with the Examiner, as an enhancement of security on an IC to allow the addition of programs by not only the original manufacture of the IC card but also authorized users and distributors of the IC card. Hirokawa does not provide any such enhanced security with respect to the addition of programs as is quite clear in the second embodiment illustrated in Figs. 19-24 of Hirokawa. Since no security is provided in the second embodiment, apparently Hirokawa contemplates that the addition of programs would only be conducted by the manufacturer of the IC card. Appellants' invention allows for addition of programs to be performed by authorized users and distributors of the IC card, other than the original manufacturer of the IC card. Since the right to add programs have been opened up to encompass other authorized users according to the present invention, the need for security increases. Allowing users other than the original manufacturer to add programs in a secure environment according to the present invention offers the advantage of a more flexible and usable IC card that is not possible in Hirokawa.

**SUMMARY**

Appellants' submit that the Examiner's rejection of claims 20-38, 51-58, 71-87, 93 and 94 as being unpatentable over Hirokawa under 35 USC §102(b) is not properly founded in law and respectfully request that the Board reverse the Examiner's rejection.

To the extent necessary, applicants petition for an extension of time under 37 C.F.R. section 1.136. Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 01-2135 (Case No. 520.38929CX2) and please credit any excess fees to such Deposit Account.

Respectfully submitted,



(703) 312-6600  
CIB/jdc

---

Carl I. Brundidge  
Registration No. 29,621  
ANTONELLI, TERRY, STOUT & KRAUS, LLP